# Chapter 21: Installing MIT Kerberos on Windows, for use with Exceed 7 and FileZilla

In this chapter we describe how to install and configure the MIT Kerberos software on your Windows system (Win2k, NT4, 95, or 98). This software, when used with the Hummingbird Exceed 7.0 telnet client and the FileZilla FTP client, allows you to authenticate to Kerberos, open Kerberized connections to remote machines, and encrypt your data transmissions. The MIT Kerberos software for Windows systems comes with a GUI called **Leash32**.

Note that while the configuration described in this chapter complies with the Fermilab Policy on Computing and some divisions are recommending and supporting it, it is not formally supported by the Computing Division.

## 21.1 Getting Ready

### 21.1.1 Obtain a Kerberos Principal

First, verify that you have administrator privileges on the PC. Next, you need to obtain a Kerberos principal and initial password for the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal*. Use the online *Request Form for Computing Username and Primary Accounts* at `http://www.fnal.gov/cd/forms/acctreq.html`.

### 21.1.2 Install Exceed and FileZilla

#### Exceed 7.0[1]

Exceed is a licensed product. We do not describe the installation process in this document. Versions prior to 7 do not support Kerberos. Version 7.0.0.0 must be patched, since it has a number of severe bugs. You can check the

1. The Exceed version information presented here was taken from the Beams Division documentation at `http://www-bdnew.fnal.gov/network/latest-software-versions.htm`.

Exceed version number by starting Exceed. The startup screen shows 7.0.0.0 for unpatched systems. The correct version shows 7.0.0.12 when starting Exceed, and 7.0.0.5 when starting Exceed host explorer.

Hummingbird Exceed 7.0 FTP connections cannot be Kerberized.

### FileZilla 1.93

FileZilla is a small (791k) but powerful freeware FTP client that supports Kerberos (as well as firewalls and proxy connections). It claims to work on virtually all the Windows platforms: W2k/NT/9x/ME/XP. The software includes a site manager to store all your connection details and logins as well as an Explorer-style interface that shows the local and remote folders and can be customized independently. Additional features include keep alive and auto ascii/binary transfer.

Download the software from `\\Pckits\PC_Tools\Apps\FileZilla_1.6\FileZilla_1_6setup.exe`. Instructions are provided in the same directory. We do not describe the installation process in this document. However, we want to draw your attention to a couple of configuration issues. Under **EDIT > SETTINGS > CONNECTION >**

- **GSS SUPPORT**: Check `Enable Kerberos GSS support`, and add `FNAL.GOV` to the **GSS ENABLED SERVERS** list (you can remove `mit.edu`).
- **FIREWALL SETTINGS**: Check `Passive Mode`

## 21.1.3 Caveats

Although it appears that you can use **Leash32** to configure Kerberos for multiple realms, we have only gotten this software to work reliably when configured for accessing a single realm.

As mentioned above, Hummingbird Exceed 7.0 FTP connections cannot be Kerberized; use FileZilla's FTP client.

# 21.2 Installing Kerberos

1) Log into an account with administrator privileges.

2) Download the Kerberos client software from MIT. First browse to: `http://web.mit.edu/network/kerberos-form.html`.

This brings you to the **Kerberos Distribution Authorization Form**. Answer the three questions, and submit the form to arrive at the download page, **Welcome to the MIT Kerberos Distribution Page!**. Scroll down (about half-way) to the section on *MIT Kerberos for Windows 2.1* and click on the file listed next to KfW 2.1 Installer (it is currently called `kfw-2.1-installer.exe`). Save the file to disk. The default location it chooses is `C:\Program Files\Accessories`.

3) Once this file is copied on to your machine, execute it to install the Kerberos program. You will be asked a series of questions, but you can safely use the defaults, and just click through the screens. Checking the time synchronization when prompted is a good idea. The software gets installed under `C:\Program Files\Kerberos` by default.

4) After installing the files, it will ask if it's OK to restart your computer. Say yes.

## 21.3 Configuring Kerberos using Leash32

1) Log back on to the same account.

2) Create the configuration file `krb5.ini` as listed in section 21.6 *krb5.ini for FNAL.GOV*, and put it in your Kerberos folder. (If you accepted the default installation values, this folder is under `C:\Program Files`.) The `krb5.ini` file is comparable to the `krb5.conf` on UNIX.

3) Find where **Exceed 7** has installed the file `krbv4w32.dll` (should be the Kerberos folder), and delete this file.

4) Navigate to **START** > **PROGRAMS** > **KERBEROS UTILITIES** > **LEASH32**. (**Leash32** is a GUI for your Kerberos client.)

5) On the **LEASH32** window, go to the **OPTIONS** menu and select **KERBEROS PROPERTIES**.

6) Under **TICKET LIFETIME**, choose how long you would like your tickets to last (in minutes). 1500 is a good choice. The rest of the configuration under this heading is done for you.

7) Back on the **LEASH32** window, go to the **OPTIONS** menu and select **KERBEROS V5 PROPERTIES**. Under the *Configuration Options* tab, check **FORWARDABLE** to make your Kerberos tickets forwardable to remote Kerberized hosts. Under the *File Location* tab, check that the configuration file path is correct.

8) Also on the **OPTIONS** menu, select **DESTROY TICKETS/TOKENS ON EXIT**.

# 21.4 Getting a Ticket

To authenticate locally using the **Leash32** utility, select **GET TICKET(S)** on the **ACTION** menu. You will be required to enter your Kerberos password. Ignore the CRYPTOCard prompt that may follow (press **CANCEL**). You ticket will appear in the **Leash32** window. Click on the Windows Explorer-style plus signs (+) to get details.

Alternatively, you can invoke the command prompt and type **`kinit -5`** to request a ticket. You will be required to enter your Kerberos password. Ignore the CRYPTOCard prompt that may follow (just press **ENTER**). To verify the ticket and its flags, either bring up the **Leash32** window, or type **`klist -f`** at the command prompt.

# 21.5 Configuring the Exceed 7 Telnet Application

## 21.5.1 Create a new Telnet Profile for Kerberized Host

You should create one profile for each Kerberized host you wish to access.

1) Start the Exceed 7 telnet program. Navigate to **START** > **PROGRAMS** > **HUMMINGBIRD CONNECTIVITY V7.0** > **HOSTEXPLORER** > **TELNET**.

2) In the **OPEN SESSION** window, click on the icon in the upper right corner (second from right) that has the blue screen inside the box with the yellow stripe over it (Rollover text is: `Create New Profile`). Set the following values:

   a) Profile Name = any name to identify the profile (e.g., target host name)

   b) Profile Type = VT

   c) Connect by = Telnet

   d) Hostname = the fully qualified name or IP address of name of the target host (e.g., myhost.fnal.gov or 131.225.876.54)

3) Back on the **OPEN SESSION** window, right-click on the profile you just created and select **PROPERTIES**.

4) In the **SETTINGS GROUP** area of the session profile, expand the **SECURITY** folder, and select **KERBEROS**.

   a) Change the **KERBEROS VERSION** to Kerberos 5 from the pulldown menu.

   b) In the **COMMON KERBEROS OPTIONS** field, check both Authentication and Encryption.

   c) In the **KERBEROS 5 OPTIONS**, check Forwarding. If your user name on the target machine is different from your principal, enter your user name under Alternate User Name.

   d) Click **OK**.

## 21.5.2 Create a new Telnet Profile for nonKerberized Host

You should create one profile for each host you wish to access.

1) Start the Exceed 7 telnet program. Navigate to **START** > **PROGRAMS** > **HUMMINGBIRD CONNECTIVITY V7.0** > **HOSTEXPLORER** > **TELNET**.

2) In the **OPEN SESSION** window, click on the icon in the upper right corner (second from right) that has the blue screen inside the box with the yellow stripe over it (Rollover text is: `Create New Profile`). Set the following values:

   a) Profile Name = any name to identify the profile (e.g., target host name)

   b) Profile Type = VT

   c) Connect by = Telnet

   d) Hostname = the fully qualified name or IP address of name of the target host (e.g., myhost.fnal.gov or 131.225.876.54)

   e) Click **OK**.

## 21.5.3 Connect to Kerberized Host using Telnet Profile

1) On the **OPEN SESSION** window, with your new profile selected, the target host name or IP address should appear in the Host Name window. To connect, click on the **CONNECT** button. If you've preauthenticated,

you should get right in without having to provide your Kerberos password.

2) The **LEASH32** window should now show your host connection in addition to the kerberos ticket.

### 21.5.4 Connect to nonKerberized Host using Telnet Profile

On the **OPEN SESSION** window, with a nonKerberized profile selected, the target host name or IP address should appear in the Host Name window. To connect, click on the **CONNECT** button. You will need to log in normally.

## 21.6 krb5.ini for FNAL.GOV

Make sure you have tabs in front of the items in each stanza, not a series of spaces.

```
[domain_realm]

        fnal.gov = FNAL.GOV



[libdefaults]

        default_realm = FNAL.GOV

        default_tgs_enctypes = des-cbc-crc

        default_tkt_enctypes = des-cbc-crc

        forwardable = true

        proxiable = true



[login]

        krb4_convert = true

        krb4_get_tickets = true
```

```
[realms]

        FNAL.GOV = {
                kdc = krb-fnal-1.fnal.gov:88
                kdc = i-krb-7.fnal.gov:88
                kdc = krb-fnal-2.fnal.gov:88
                kdc = krb-fnal-3.fnal.gov:88
                kdc = krb-fnal-4.fnal.gov:88
                kdc = krb-fnal-5.fnal.gov:88
                admin_server = krb-fnal-admin.fnal.gov
                default_domain = fnal.gov        }
```